XACML 3.0 Intellectual Property Control (IPC) Profile Version 1.0

Committee Draft 01

10 September 2009

Specification URIs:
This Version:

Previous Version:
N/A

Latest Version:
http://docs.oasis-open.org/xacml/3.0/ipc/xacml-3.0-ipc-v1-spec-en.doc (Authoritative)
http://docs.oasis-open.org/xacml/3.0/ipc/xacml-3.0-ipc-v1-spec-en.html

Technical Committee:
OASIS eXtensible Access Control Markup Language (XACML) TC

Chair(s):
Bill Parducci, <bill@parducci.net>
Hal Lockhart, Oracle <hal.lockhart@oracle.com>

Editor(s):
John Tolbert, The Boeing Company

Related work:
This specification is related to:
- eXtensible Access Control Markup Language (XACML)

Abstract:
This specification defines a profile for the use of XACML in expressing policies for intellectual
property control (IPC). It defines standard attribute identifiers useful in such policies, and
recommends attribute value ranges for certain attributes.

Status:
This document was last revised or approved by the eXtensible Access Control Markup Language
(XACML) TC on the above date. The level of approval is also listed above. Check the "Latest
Version" or "Latest Approved Version" location noted above for possible later revisions of this
document.

Technical Committee members should send comments on this specification to the Technical
Committee’s email list. Others should send comments to the Technical Committee by using the
“Send A Comment” button on the Technical Committee’s web page at http://www.oasis-
open.org/committees/xacml/.

For information on whether any patents have been disclosed that may be essential to
implementing this specification, and any offers of patent licensing terms, please refer to the

The non-normative errata page for this specification is located at http://www.oasis-open.org/committees/xacml/.
Notices

Copyright © OASIS® 2009. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The names "OASIS", [insert specific trademarked names and abbreviations here] are trademarks of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see http://www.oasis-open.org/who/trademark.php for above guidance.
# Table of Contents

1   Introduction ................................................................................................................................. 5  
1.1  Glossary .................................................................................................................................. 6  
1.2  Terminology .............................................................................................................................. 7  
1.3  Normative References ............................................................................................................... 7  
1.4  Non-Normative References ...................................................................................................... 7  
1.5  Scope .......................................................................................................................................... 7  
1.6  Use cases ................................................................................................................................... 8  
1.7  Disclaimer ................................................................................................................................. 8  
2   Profile .......................................................................................................................................... 9  
2.1  Resource Attributes ................................................................................................................... 9  
2.1.1 IPC-Type ................................................................................................................................. 9  
2.1.2 IPC-Data .................................................................................................................................. 9  
2.1.3 IP-Owner ............................................................................................................................... 9  
2.1.4 IP-Designee ............................................................................................................................ 9  
2.1.5 EC-US ..................................................................................................................................... 9  
2.1.6 License ................................................................................................................................... 9  
2.2  Subject Attributes ..................................................................................................................... 10  
2.2.1 Nationality ............................................................................................................................ 10  
2.2.2 Organization .......................................................................................................................... 10  
2.3  Environment Attributes ......................................................................................................... 10  
2.3.1 Location .................................................................................................................................. 10  
2.4  Action Attributes ...................................................................................................................... 10  
2.4.1 Storage ................................................................................................................................... 10  
2.4.2 Physical transmission ............................................................................................................. 10  
2.4.3 Electronic transmission .......................................................................................................... 10  
2.4.4 Encryption type ..................................................................................................................... 11  
2.4.5 Marking .................................................................................................................................. 11  
2.4.6 Disposal .................................................................................................................................. 11  
2.4.7 Authority ............................................................................................................................... 11  
3   Identifiers ..................................................................................................................................... 12  
3.1  Profile Identifier ....................................................................................................................... 12  
4   Conformance ................................................................................................................................. 13  
4.1  Introduction ............................................................................................................................... 13  
4.2  Conformance tables .................................................................................................................. 13  
4.2.1 Attributes .............................................................................................................................. 13  
A.  Acknowledgements ..................................................................................................................... 14  
B.  Non-Normative Text ................................................................................................................... 14  
C.  Revision History .......................................................................................................................... 15
1 Introduction

{Non-normative}

This specification defines a profile for the use of the OASIS eXtensible Access Control Markup Language (XACML) to write and enforce policies for the purpose of providing access control for resources deemed intellectual property (hereinafter referred to as IP). Use of this profile requires no changes or extensions to the XACML standard.

This specification begins with a non-normative discussion of the topics and terms of interest in this profile. The normative section of the specification describes the attributes defined by this profile and provides recommended usage patterns for attribute values.

This specification assumes the reader is somewhat familiar with XACML. A brief overview sufficient to understand these examples is available in [XACMLIntro].

For our purposes, IP may be defined as legal property rights over mental creations. IP owners can receive exclusive rights to their creations, if certain conditions are met. These exclusive rights can be exploited by the owner for profit, either directly through sales of products, or indirectly through licensing.

IP is an asset; perhaps the most valuable asset an organization has. IP can be licensed to other organizations in cases of outsourcing and/or to generate revenue from IP sharing arrangements.

IP value tends to increase when properly protected, though there are differing points of diminishing returns. IP protection doesn’t guarantee security; it just provides a compensation mechanism for cases of unlawful exploitation. IP valuation and protection are often criteria for venture capital investors.

Broadly speaking, there are four main categories of intellectual property: copyrights, trademarks, trade secrets, and patents. Copyrights confer time-limited exclusive rights of ownership and/or use to the creator of the work. A copyright is typically used to protect artistic works such as photographs, music, books, etc. Copyrights are internationally recognized, though there are differences in the terms and enforcement.

Trademarks are the IP protection scheme of names, logos, symbols, products, etc. For example, in the U.S. there are 2 main types:

- For general usage, or for not-yet-registered trademarks ™
- For trademarks registered with the USPTO ®

Trademarks are also internationally recognized through the Madrid system, which requires registration through the World Intellectual Property Organization (WIPO), a United Nations agency. The World Trade Organization also sets legal minimum standards for IP protection among member nations.

Patents are property rights granted to an inventor to prevent others from profiting from the invention for a limited time in exchange for public disclosure of the invention when the patent is granted. Patents apply to processes, machines, articles of manufacture, or composition of matter (including biological), or derived innovations. Patents require detailed disclosure of information, designs, processes, etc. Patents are administered in U.S. by the USPTO, and are internationally recognized by WTO TRIPS, WIPO, and European Patent Convention.

Trade secrets are IP protection of formulae, processes, designs, information, etc. that are not easily obtainable that a business uses for competitive advantage. They are often protected by legal contracts such as non-disclosure agreements, non-compete agreements, or proprietary information agreements.

Trade secrets are the most common form of industrial IP protection, and outnumber patents. However, trade secrets are often categorized as “proprietary” information, and may not be discovered as trade secrets unless litigated. They are not federally protected in the U.S., though most states have adopted the Uniform Trade Secrets Act. However, theft of trade secrets is prohibited by U.S. Economic Espionage Act of 1996. Trade secret status requires less disclosure than patents. Trade secrets are well protected by European Patent Convention as “know how”. No international treaties protect trade secrets, though WTO TRIPS, GATT, and NAFTA have provisions for trade secret protection.

Other IP related concepts, such as public domain, PII, proprietary, and third-party proprietary will be defined in the glossary section.
The attributes and glossary terms defined below are not an exclusive or comprehensive list of all the attributes that may be required for rendering authorization decisions concerning IP. For example, PDPs would have to evaluate other entitlements, such as group membership, from PIPs. This profile is meant as a point of reference for implementing IP controls, and may be extended as needed for organizational purposes. Software vendors who choose to implement this profile should take the attributes herein as a framework for IP controls, but allow individual implementers some flexibility in constructing their own XACML-based authorization policies and PDPs.

The goal of this profile is to create a framework of common IP-related attributes upon which authorization decisions can be rendered. This profile will also provide XACML software developers and authorization policy writers guidance on supporting IP control use cases.

1.1 Glossary

Authority

The entity which is responsible for authorizing the transaction. This can be a particular company, organization, or contract.

Copyright

A form of limited and temporary government-granted monopoly which gives the creator of an original work some rights for a certain time period in relation to that work, including its publication, distribution and adaptation; after which time the work is said to enter the public domain. Copyright applies to concrete expressions of information, but not the information itself.

Country

A national political administrative unit recognized for diplomatic and trade purposes by governments and other international organizations.

EAR

Export Administration Regulations, US laws and regulations administered by the Department of Commerce.

IP-Designee

A designation for the persons or entities with designated intellectual property rights.

IP-Owner

A designation for the entity which owns the intellectual property.

ITAR

International Traffic in Arms Regulations; USA laws and regulations administered by the Department of State.

License

An agreement granting rights in Intellectual Property.

Location

The location of the requesting principal. Values of acceptable locations may be specified by legal contract, and may be specific to implementations. PDPs and PEPs SHOULD be configured for mutual understanding of said values.

Nationality

A country of which a person is a citizen.

Organization

A company or other legal entity of which a person can be an employee or agent.

Patent

A set of exclusive rights granted by a government to an inventor or his assignee for a limited period of time in exchange for a disclosure of an invention.
PII
Personally identifiable information. For example, U.S. Social Security Numbers.

Proprietary
Information protected by an organization by technical controls. May sometimes be used synonymously with "trade secret".

Public domain (PUB)
Information that has been demoted from copyright, trademark, trade secret, or patented status.
No intellectual property controls are usually necessary for items considered public domain.

Third-party proprietary
Intellectual property which has been legally entrusted to the care and use of another organization.

Trademark
A distinctive sign or indicator used by an individual, business organization, or other legal entity to identify that the products, and/or services to consumers with which the trademark appears originate from a unique source of origin, and to distinguish its products or services from those of other entities.

Trade secret
A formula, practice, process, design, instrument, pattern, or compilation of information which is not generally known or reasonably ascertainable, by which a business can obtain an economic advantage over competitors or customers. In some jurisdictions, such secrets are referred to as "confidential information" or "classified information".

1.2 Terminology
The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

1.3 Normative References


1.4 Non-Normative References


1.5 Scope
Many intellectual property access control decisions can be made on the basis of the resource’s copyright, trademark, patent, trade secret, or other custom classification. This profile defines standard XACML attributes for these properties, and recommends the use of standardized attribute values.

In practice, an organization’s intellectual property protection policies will be a mixture of rules derived from laws and regulations, along with enterprise-specific rules derived from government-approved bilateral or multilateral agreements with other organizations.
1.6 Use cases

PDPs may need to consider intellectual property protection schemes when evaluating authorization decisions. This profile is designed to provide a framework of additional <Attributes> for such decisions.

Copyright use case: an authorization decision depends on whether or not the resource in question is protected by copyright.

Trademark use case: an authorization decision depends on whether or not the resource in question is a designated trademark.

Patent use case: an authorization decision depends whether or not the resource in question is protected by a patent. Patent designation may follow.

Trade secret use case: an authorization decision depends whether or not the resource in question is designated as a trade secret.

PII use case: an authorization decision depends whether or not the resource in question is designated as personally identifiable information.

Third-party proprietary: an authorization decision depends whether or not the resource in question is designated as a third-party proprietary resource.

License: a calling PEP may need to log that a particular license applies to the authorization decision rendered by the PDP.

1.7 Disclaimer

NOTHING IN THIS PROFILE IS INTENDED TO BE A LEGALLY CORRECT INTERPRETATION OR APPLICATION OF U.S. OR ANY GOVERNMENT INTELLECTUAL PROPERTY LAWS OR REGULATIONS. USE OF THIS PROFILE IN AN ACCESS CONTROL SYSTEM DOES NOT CONSTITUTE COMPLIANCE WITH ANY INTELLECTUAL PROPERTY RESTRICTIONS. THIS PROFILE HAS NOT BEEN REVIEWED OR ENDORSED BY THE U.S. OR ANY OTHER GOVERNMENT AGENCIES RESPONSIBLE FOR ENFORCING INTELLECTUAL PROPERTY LAWS, NOR BY ANY LEGAL EXPERT IN THIS FIELD.

Organizations that use this profile should ensure their intellectual property protection by engaging qualified professional legal services.
2 Profile

2.1 Resource Attributes

2.1.1 IPC-Type

The IPC-Type classification value shall be designated with the following attribute identifier:

\text{urn:oasis:names:tc:xacml:3.0:ipc:resource:ipc-type}

The \textit{DataType} of this attribute is \texttt{http://www.w3.org/2001/XMLSchema#string}. Examples of acceptable values of the attribute SHALL be “PUB”, “PII”, “EC-US”, “COPYRIGHT”, “TRADEMARK”, “PATENT”, “TRADESECRET”, “PROPRIETARY”, or “THIRD-PARTY PROPRIETARY”. Other values may also be defined later, depending on an organization’s authorization needs.

The use of “THIRD-PARTY PROPRIETARY” may introduce ambiguity in a federated authorization model. In that case, “PROPRIETARY” with a corresponding \textit{IP-Owner} value \textbf{SHOULD} be used to distinguish IP owned by an entity other than the PDP’s home organization.

2.1.2 IPC-Data

IPC-Data classification values shall be designated with the following attribute identifier:

\text{urn:oasis:names:tc:xacml:3.0:ipc:resource:ipc-data}

The \textit{DataType} of this attribute is \texttt{http://www.w3.org/2001/XMLSchema#string}. The purpose of this attribute is to convey additional data about the intellectual property resource, such as author names, patent numbers, proprietary tracking information, etc.

2.1.3 IP-Owner

IP-Owner classification values shall be designated with the following attribute identifier:

\text{urn:oasis:names:tc:xacml:3.0:ipc:resource:ip-owner}

The \textit{DataType} of this attribute is \texttt{http://www.w3.org/2001/XMLSchema#string}. This attribute names the owner of the IP.

2.1.4 IP-Designee

IP-Designee classification values shall be designated with the following attribute identifier:

\text{urn:oasis:names:tc:xacml:3.0:ipc:resource:ip-designee}

The \textit{DataType} of this attribute is \texttt{http://www.w3.org/2001/XMLSchema#string}. This attribute names the designated custodian of the IP.

2.1.5 EC-US

EC-US classification values shall be designated with the following attribute identifier:

\text{urn:oasis:names:tc:xacml:3.0:ipc:resource:ec-us}

The \textit{DataType} of this attribute is \texttt{http://www.w3.org/2001/XMLSchema#string}. This attribute can contain export control data related to the EC-US profile. If the IP resource is also export-controlled, it can be indicated here, and invoke the EC-US determination as needed. The attribute could also contain the result of an EC-US decision.

2.1.6 License

License classification values shall be designated with the following attribute identifier:
The DataType of this attribute is http://www.w3.org/2001/XMLSchema#string. This attribute can be used to indicate whether or not a specific resource is governed by a particular license arrangement.

2.2 Subject Attributes

2.2.1 Nationality

Nationality classification values shall be designated with the following attribute identifier:

urn:oasis:names:tc:xacml:3.0:ipc:subject:nationality

The DataType of this attribute is http://www.w3.org/2001/XMLSchema#string. The value of this attribute MUST be in the range of 2-letter country codes defined by [ISO3166]. Nationality shall denote the country in which the subject currently has legal status as a “national” or citizen.

2.2.2 Organization

Organization classification values shall be designated with the following attribute identifier:

urn:oasis:names:tc:xacml:3.0:ipc:subject:organization

The DataType of this attribute is http://www.w3.org/2001/XMLSchema#string. Organization shall denote the organization to which the subject in the request belongs. A common scheme such as DUNS SHOULD be used to promote interoperability.

2.3 Environment Attributes

2.3.1 Location

Location classification values shall be designated with the following attribute identifier:

urn:oasis:names:tc:xacml:3.0:ipc:environment:location

The DataType of this attribute is http://www.w3.org/2001/XMLSchema#string.

2.4 Action Attributes

2.4.1 Storage

Storage classification values shall be designated with the following attribute identifier:

urn:oasis:names:tc:xacml:3.0:ipc:action:storage

The DataType of this attribute is http://www.w3.org/2001/XMLSchema#string.

2.4.2 Physical transmission

Physical transmission classification values shall be designated with the following attribute identifier:

urn:oasis:names:tc:xacml:3.0:ipc:action:physical-transmission

The DataType of this attribute is http://www.w3.org/2001/XMLSchema#boolean.

2.4.3 Electronic transmission

Electronic transmission classification values shall be designated with the following attribute identifier:


The DataType of this attribute is http://www.w3.org/2001/XMLSchema#string.
### 2.4.4 Encryption type

Encryption type classification values shall be designated with the following attribute identifier:

```xml
urn:oasis:names:tc:xacml:3.0:ipc:action:encryption-type
```

The **DataType** of this attribute is `http://www.w3.org/2001/XMLSchema#string`.

### 2.4.5 Marking

Marking classification values shall be designated with the following attribute identifier:

```xml
urn:oasis:names:tc:xacml:3.0:ipc:action:marking
```

The **DataType** of this attribute is `http://www.w3.org/2001/XMLSchema#string`. Examples of marks could be "Proprietary", "Confidential", etc.

### 2.4.6 Disposal

Disposal classification values shall be designated with the following attribute identifier:

```xml
urn:oasis:names:tc:xacml:3.0:ipc:action:disposal
```

The **DataType** of this attribute is `http://www.w3.org/2001/XMLSchema#string`.

### 2.4.7 Authority

Authority classification values shall be designated with the following attribute identifier:

```xml
urn:oasis:names:tc:xacml:3.0:ipc:action:authority
```

The **DataType** of this attribute is `http://www.w3.org/2001/XMLSchema#string`.

This attribute can be used to describe the associated contract or statement of work authorizing the access. Other types of values could be used depending on an organization's needs.
This profile defines the following URN identifiers.

### 3.1 Profile Identifier

The following identifier SHALL be used as the identifier for this profile when an identifier in the form of a URI is required.

```plaintext
urn:oasis:names:tc:xacml:3.0:profiles:ipc
```
4 Conformance

Conformance to this profile is defined for policies and requests generated and transmitted within and between XACML systems.

4.1 Attribute Identifiers

Conformant XACML policies and requests SHALL use the attribute identifiers defined in Section 2 for their specified purpose.

4.2 Attribute Values

Conformant XACML policies and requests SHALL use attribute values in the specified range or patterns as defined for each attribute in Section 2 (when a range or pattern is specified).

NOTE: In order to process conformant XACML policies and requests correctly, PIP and PEP modules may have to translate native data values into the datatypes and formats specified in this profile.
A. Acknowledgements

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

**Participants:**
- John Tolbert, The Boeing Company

**Committee members during profile development:**

- Erik Rissanen, Axiomatics AB
- Ludwig Seitz, Axiomatics AB
- Paul Tyson, Associate
- Ronald Jacobson, CA
- Masum Hasan, Cisco Systems, Inc.
- Anil Tappetla, Cisco Systems, Inc.
- Tim Moses, Entrust
- Guy Denton, IBM
- Craig Forster, IBM
- Richard Franck, IBM
- Michiharu Kudo, IBM
- Michael McIntosh, IBM
- Vernon Murdoch, IBM
- Ron Williams, IBM
- David Chadwick, Individual
- Bill Parducci, Individual
- Harry Haury, NuParadigm Government Systems, Inc.
- Kamalendu Biswas, Oracle Corporation
- Willem de Pater, Oracle Corporation
- Rich Levinson, Oracle Corporation
- Hal Lockhart, Oracle Corporation
- Prateek Mishra, Oracle Corporation
- Anil Saldhana, Red Hat
- Darran Rolls, SailPoint Technologies
- Dilli Arumugam, Sun Microsystems
- Seth Proctor, Sun Microsystems
- Aravindan Ranganathan, Sun Microsystems
- John Tolbert, The Boeing Company
- Martin Smith, US Department of Homeland Security
- Duane DeCouteau, Veterans Health Administration
- David Staggs, Veterans Health Administration
## B. Revision History

[optional; should not be included in OASIS Standards]

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Editor</th>
<th>Changes Made</th>
</tr>
</thead>
<tbody>
<tr>
<td>CD 1</td>
<td>6/18/09</td>
<td>John Tolbert</td>
<td>Initial committee draft.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>